UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,476	08/13/2001	Luu Tran	SUN-P6088	9070

32615 7590 01/13/2005

OSHA & MAY L.L.P./SUN
1221 MCKINNEY, SUITE 2800
HOUSTON, TX 77010

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/929,476	TRAN ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-26 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-26 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 13 August 2001 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 1-26 are pending.

Double Patenting

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claim 1 is provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of copending Application No. 09/929477. Although the conflicting claims are not identical, they are not patentably distinct from each other because narrower claim 1 of the copending application renders the broader claim of this application obvious.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) for the following reasons:

- Reference numbers 211, 212, and 213 of Figure 2 are not referred to in the specification.
- Reference numbers 315 and 325 of Figure 3 are not referred to in the specification.
- Reference numbers 325 and 360 have both been used to designate the client data module.
- Reference number 315 is used in the drawings to designate the client detection module, but is referred to as 350 in the specification.
- Reference number 350 in Figure 3 is used to designate a logging service, which is not discussed in the specification.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

2. The disclosure is objected to because of the following informalities:

- Page 13, line 3: "in native" should be "in the native".
- Page 13, line 13: "protocol shown" should be "protocols shown".
- Page 14, line 1: "is a flexible" should be "is flexible".
- Page 14, line 19: "independent wireless devices" should be "an independent wireless device".
- Page 15, line 5: "filed_____" should contain the date the copending application was filed on.
- Page 16, line 9: "includes client's" should be "include client's".
- Page 16, line 16: "authenticating services 310" should be "authenticating service 310".

Appropriate correction is required.

Claim Objections

3. Claims 2, 3, 8, 13, 17, and 25 are objected to under 37 CFR 1.75(a) because of the following informalities:

- Claim 2, line 1: "comprises" should be "comprising".
- Claim 3, line 3 recites the limitation "the authentication characteristics". There is insufficient antecedent basis for this limitation in the claims. For

purposes of prior art rejections, it has been construed as "authentication characteristics".

- Claim 8, line 1: "A wireless server system" should be "The wireless server system".
- Claim 13, line 7: "modules" should be "module".
- Claim 17, line 1: "wireless server system" should be "wireless server".
- Claim 17, line 2: "data storage" should be "data storage module".
- Claim 17, line 3: "client type value" should be "client type information".
- Claim 17, line 3: "the session service logic" should be "the session service module".
- Claim 25, line 4: "module" should be "modules".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by O'Shea et al. (U.S. Patent Application Publication 2002 0,152,380).

A client aware authentication system in a wireless network, comprising:

A wireless server [recipient of the parameter update message] (Detailed Description, Paragraph 29); and

A plurality of classes of wireless clients, each of the classes of wireless clients having unique authentication parameters (Detailed Description, Paragraph 24).

5. Claims 24-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Stoltz et al. (U.S. Patent 6,615,264).

Regarding Claim 24,

A client aware authentication module, comprising:

A plurality of characteristics modules (Column 17, lines 7-37); and

Client aware authentication selection logic (Column 8, lines 57-65).

Regarding Claim 25,

The plurality of client aware characteristics modules comprise a predefined set of client characteristics for authenticating known clients accessing the client aware authentication module (Column 10, lines 2-5).

Regarding Claim 26,

The plurality of client aware characteristics modules comprise client characteristics dynamically extracted from the clients run-time environment (Column 17, lines 26-37).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'Shea et al. (U.S. Patent Application Publication 2002 0,152,380) in view of Stoltz et al. (U.S. Patent 6,615,264).

Regarding Claim 2,

O'Shea et al. do not disclose the use of an authentication service to decide which authentication module to send an authentication request to.

Stoltz et al., however, disclose a client aware authentication system comprising a plurality of authentication modules coupled to an authentication service [authentication manager] and wherein the authentication service is for dynamically selecting an authentication service module based on the class of a client (Column 8, lines 48-56). This new system would be the system from above using an authentication service to determine which authentication module to use to authenticate the client.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use an authentication service in such a way

in order to distribute the authentication load. One of ordinary skill in the art would have been motivated to do so in order to allow each authentication module to handle authenticating clients of a different class, or of multiple classes (Column 8, lines 57-65).

Regarding Claim 3,

O'Shea et al. disclose that the authentication service receives and parses client type information of the wireless clients to determine authentication characteristics of the wireless client (Detailed Description, Paragraph 30).

Regarding Claim 4,

The system from above discloses a wireless server and clients, but does not disclose what the authentication modules comprise.

Stoltz et al., however, disclose that the plurality of authentication modules comprises a set of predefined authentication parameters used by the server to authenticate the clients with known authentication characteristics accessing the server (Column 9, lines 19-26). This new system would be the system from above having each authentication module structured in a predefined way.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to structure the authentication modules in order to allow different authentication modules to authenticate different classes of client but still communicate with the server in a predefined

manner. One of ordinary skill in the art would have been motivated to do so in order to allow uniform communication with the server, while giving the authentication modules authority to authenticate clients in a different manner, depending on the situation.

Regarding Claim 5,

The system from above does not disclose that the authentication module comprises parameters extracted from the client information.

Stoltz et al., however, disclose that the authentication module further comprises authentication parameters dynamically extracted from client type information of the clients accessing the server (Column 9, lines 35-46). This new system would be the system from above using client information sent in the authentication request in order to authenticate the client.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use client parameters in the authentication module in order to create an authenticated session. One of ordinary skill in the art would have been motivated to do so in order to form a session specific to the client upon proper authentication.

Regarding Claim 6,

The system from above does not disclose that the authentication module provides information to the authentication server.

Stoltz et al., however, disclose that the authentication module selectively provides client specific authentication information to the authentication server in order to authenticate the clients accessing the server (Column 9, line 65 to Column 10, line 5). This new system would be the system from above allowing the authentication modules to send certain authentication information to the authentication server.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to selectively provide client specific authentication information from the authentication module to the authentication server in order to lighten the authentication load the next time the same client wishes to authenticate itself. One of ordinary skill in the art would have been motivated to do so in order to allow for an authentication module that authenticates quickly using this stored information.

Regarding Claim 7,

O'Shea et al. disclose a system including a wireless server [recipient of the parameter update message] (Detailed Description, Paragraph 29) and a plurality of wireless clients (Detailed Description, Paragraph 22).

O'Shea et al. do not disclose client authentication at different authentication modules.

Stoltz et al., however, disclose a server system comprising:

A plurality of authentication modules each providing respective authentication parameters pertinent to a type of client (Column 9, lines 19-26); and

An authentication service, in response to receiving a particular client type associated with a particular device, for dynamically selecting an authentication module of the plurality of authentication modules based on the particular client type (Column 8, lines 48-56),

Wherein the authentication service is also for applying a selected authentication module to the particular device for the authentication thereof (Column 8, lines 54-56).

This new system would be the system from O'Shea et al. using an authentication service to determine which of the plurality of authentication modules to send the client's authentication request to.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use an authentication with the plurality of authentication modules in this way in order to distribute the authentication load. One of ordinary skill in the art would have been motivated to do so in order to allow each authentication module to handle authenticating clients of a different class, or of multiple classes (Column 8, lines 57-65).

7. Claims 8-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'Shea et al. (U.S. Patent Application Publication 2002 0,152,380) in view of Stoltz et al. (U.S. Patent 6,615,264), further in view of Liao et al. (U.S. Patent 6,606,663).

Regarding Claim 8,

The system from above does not disclose a service for detecting the client type.

Liao et al., however, disclose an automatic client detection service for automatically detecting the particular client type in response to service requests that originate from the particular wireless device (Column 7, lines 55-61). This new system would be the system from above detecting the client type at the authentication service.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to detect what type of client was sending the request in order to allow for proper authentication of the device. One of ordinary skill in the art would have been motivated to do so in order to obtain the client's credentials so as to allow for authentication of the device.

Regarding Claim 9,

The system from above does not disclose the use of headers for detecting the client type.

Liao et al. disclose that the service requests comprise header information which is used to detect the particular client type (Column 7,

lines 55-61). This new system would be the system from above detecting the client type through headers.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to detect the client type through the header in order to allow for proper authentication of the device. One of ordinary skill in the art would have been motivated to do so in order to obtain the client's credentials so as to allow for authentication of the device.

Regarding Claim 10,

The system from above does not disclose the use of HTTP headers.

Liao et al., however, disclose that the header information comprises hypertext transport protocol request headers (Column 7, lines 7-25). This new system would be the system from above using HTTP headers to communicate between the client device and the server.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use HTTP headers during authentication in order to allow for more devices to use the system. One of ordinary skill in the art would have been motivated to do so in order to client devices that utilize HTTP to use the system.

8. Claims 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'Shea et al. (U.S. Patent Application Publication 2002 0,152,380) in view of Stoltz

et al. (U.S. Patent 6,615,264) and Liao et al. (U.S. Patent 6,606,663), further in view of Jacklin et al. (U.S. Patent 6,169,730).

Regarding Claim 11,

The system from above does not disclose programmable user specific headers.

Jacklin et al., however, disclose that the header information comprises programmable user specific headers (Column 5, lines 38-46 and Column 12, lines 40-50). This new system would be the system from above including a header field that is programmable by the user.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a programmable user specific header field in order to allow for communications when a client is too far away from the wireless transmitter. One of ordinary skill in the art would have been motivated to do so in order to allow a client that is too far away from the wireless transmitter to still communicate with it through other clients that are closer to the transmitter (Column 5, lines13-37).

Regarding Claim 12,

The system from above does not disclose that the headers are specified by the manufacturer of the client device.

Liao et al., however, disclose that the header information comprises client equipment manufacturer specified headers (Column 5, lines 23-36).

This new system would be the system from above using headers set by the manufacturer of the client device.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use such manufacturer specified headers in order to allow for compatibility with readily available headers. One of ordinary skill in the art would have been motivated to do so in order to obtain compatibility with widely used clients.

9. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over O'Shea et al. (U.S. Patent Application Publication 2002 0,152,380) in view of Stoltz et al. (U.S. Patent 6,615,264) and Liao et al. (U.S. Patent 6,606,663), further in view of Suzuki et al. (U.S. Patent Application Publication 2001 / 0,056,413), Wu et al. (U.S. Patent 5,774,551), TAOS Glossary (05/2000), and Durst et al. (U.S. Patent 6,434,561).

The system from above does not disclose user identification, password, membership, securID, safeword, S/key, Microsoft Windows/NT, or nopassword modules.

Stoltz et al., however, disclose a user identification module (Column 9, lines 27-30), a password module (Column 9, lines 19-22), a Microsoft Windows/NT module (Column 6, lines 11-27), and a nopassword module (Column 8, lines 7-16). This new system would be the system from above further comprising those four modules.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to have these modules in order to increase the compatibility of the server system. One of ordinary skill in the art would have been motivated to do so in order to allow clients using these protocols to authenticate through the server system.

The system from above does not disclose membership, securID, safeword, or S/key modules.

Suzuki et al., however disclose a membership module (Detailed Description, Paragraph 263). This new system would be the system from above further comprising a membership module.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to have a membership module in order to increase the compatibility of the server system. One of ordinary skill in the art would have been motivated to do so in order to allow clients using a membership protocol to authenticate through the server system.

The system from above does not disclose securID, safeword, or S/key modules.

Wu et al., however, disclose a securID module (Column 15, lines 54-63). This new system would be the system from above further comprising a securID module.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to have a securID module in order to increase the

compatibility of the server system. One of ordinary skill in the art would have been motivated to do so in order to allow clients using the securID protocol to authenticate through the server system.

The system from above does not disclose safeword or S/key modules.

TAOS Glossary, however, discloses a safeword module (Page 192, Paragraphs 4-5). This new system would be the system from above further comprising a safeword module.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to have a safeword module in order to increase the compatibility of the system. One of ordinary skill in the art would have been motivated to do so in order to allow clients using the safeword protocol to authenticate through the server system.

The system from above does not disclose a S/key module.

Durst et al., however, disclose a S/key module (Column 9, lines 16-30). This new system would be the system from above further comprising a S/key module.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to have a S/key module in order to increase the compatibility of the server system. One of ordinary skill in the art would have been motivated to do so in order to allow clients using the S/key protocol to authenticate through the server system.

10. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over O'Shea et al. (U.S. Patent Application Publication 2002 0,152,380) in view of Stoltz et al. (U.S. Patent 6,615,264), Liao et al. (U.S. Patent 6,606,663), Suzuki et al. (U.S. Patent Application Publication 2001 / 0,056,413), Wu et al. (U.S. Patent 5,774,551), TAOS Glossary (05/2000), and Durst et al. (U.S. Patent 6,434,561), further in view of Blanco (U.S. Patent 6,539,482).

The system from above does not disclose UNIX, RADIUS, or LDAP authentication modules.

Stoltz et al., however, disclose a UNIX authentication module (Column 6, lines 11-27). This new system would be the system from above further comprising a UNIX authentication module.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to have a UNIX authentication module in order to increase the compatibility of the server system. One of ordinary skill in the art would have been motivated to do so in order to allow UNIX clients to authenticate through the server system.

The system from above does not disclose RADIUS or LDAP authentication modules.

Blanco et al., however, disclose a RADIUS authentication module (Column 4, lines 42-48) and an LDAP authentication module (Column 4, lines 25-28). This new system would be the system from above further comprising a RADIUS authentication module and an LDAP authentication module.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to have a RADIUS and LDAP authentication modules in order to increase the compatibility of the server system. One of ordinary skill in the art would have been motivated to do so in order to allow RADIUS and LDAP clients to authenticate through the server system.

11. Claims 15-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Liao et al. (U.S. Patent 6,606,663) in view of Stoltz et al. (U.S. Patent 6,615,264).

Regarding Claim 15,

Liao et al. disclose a wireless server, comprising:

A client data storage module for storing client type information (Column 7, lines 51-54); and

A session service module for storing transient session information for a client requesting authentication to the wireless server (Column 10, lines 26-28).

Liao et al. do not disclose the service logic or authentication modules.

Stoltz et al., however disclose the following:

A client aware authentication service logic [authentication manager] (Column 8, lines 48-56);

A plurality of client aware authentication modules (Column 8, lines 48-56);

This new system would be the system from Liao et al. authenticating client devices through use of an authentication service logic and multiple authentication modules.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use the authentication service logic and authentication modules from Stoltz et al. in the system of Liao et al. in order to distribute the authentication load. One of ordinary skill in the art would have been motivated to do so in order to allow each authentication module to handle authenticating clients of a different class, or of multiple classes (Column 8, lines 57-65).

Regarding Claim 16,

The system from above does not disclose that the authentication service logic authenticates the clients.

Stoltz et al., however, disclose that the authentication service logic authenticates clients attempting to access the wireless server via the plurality of authentication modules (Column 9, lines 8-15). This new system would be the system from above authenticating the clients through the authentication service logic and authentication modules.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to authenticate clients through the authentication service logic in order to provide control for the authentication service logic over the authentication modules. One of

ordinary skill in the art would have been motivated to do so in order to allow the authentication service logic to control which authentication module will authenticate each client and which services to provide for the module.

Regarding Claim 17,

Liao et al. disclose that the authentication service logic retrieves client type information from the client data storage module and stores the client type information in the session service module to enable the client to be authenticated by the wireless server (Column 7, lines 26-31 and Column 7, line 67 to Column 8, line 5).

Regarding Claim 18,

Liao et al. disclose that the authentication modules comprise a set of predefined authentication parameters for authenticating known classes of wireless clients that access the wireless server (Column 7, lines 55-61).

Regarding Claim 19,

The system from above does not disclose that the authentication modules comprise parameters extracted from the service request headers.

Stoltz et al., however, disclose that the authentication modules comprise a set of dynamically extracted authentication parameters from service request headers from the wireless clients (Column 9, lines 35-46). This new system would be the system from above using client information

sent in the authentication request header in order to authentication the client.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to extract authentication parameters from the service request headers in order to create an authenticated session. One of ordinary skill in the art would have been motivated to do so in order to form a session specific to the client upon proper authentication.

Regarding Claim 20,

The system from above does not disclose that the authentication modules can choose how to authenticate the client.

Stoltz et al., however, disclose that the authentication modules comprise selection logic to selectively choose authentication parameters in response to a client service request (Column 7, line 61 to Column 8, line 2). This new system would be the system from above giving the authentication modules the decision as to how to authenticate the client.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to allow the authentication modules to choose how to authenticate the client in order to allow different authentication modules to authenticate clients with different authentication parameters. One of ordinary skill in the art would have been motivated to do so in order to have each authentication module be set for only authenticating certain authentication parameters.

Regarding Claim 21,

The system from above does not disclose the use of HTTP headers.

Liao et al., however, disclose that the client service request comprises hypertext transport protocol request headers (Column 7, lines 7-25). This new system would be the system from above using HTTP headers to communicate between the client device and the server.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use HTTP headers during authentication in order to allow for more devices to use the system. One of ordinary skill in the art would have been motivated to do so in order to client devices that utilize HTTP to use the system.

Regarding Claim 22,

Liao et al. disclose that the client service request comprises client equipment manufacturer specific headers (Column 5, lines 23-36).

12. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Liao et al. (U.S. Patent 6,606,663) in view of Stoltz et al. (U.S. Patent 6,615,264), further in view of Jacklin et al. (U.S. Patent 6,169,730).

The system from above does not disclose programmable user specified headers.

Jacklin et al., however, disclose that the client service request includes programmable user specified headers (Column 5, lines 38-46 and Column 12, lines 40-50). This new system would be the system from above including a header field that is programmable by the user.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a programmable user specific header field in order to allow for communications when a client is too far away from the wireless transmitter. One of ordinary skill in the art would have been motivated to do so in order to allow a client that is too far away from the wireless transmitter to still communicate with it through other clients that are closer to the transmitter (Column 5, lines13-37).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free)..

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER